

Serial No. 09/607007

- 24 -

Art Unit:2143

REMARKS

Reconsideration and further examination is respectfully requested.

Rejections under 35 U.S.C. §102

Claims 1-152 were rejected under 35 U.S.C. §102(b) as being anticipated by Mitra, U.S. Patent 5,748,736.

It is noted that in order to support a rejection under 35 U.S.C. §102, every limitation in the claim must be found or suggested in the prior art. As will be described below, the key distribution scheme described in Mitra is different than that recited in the claimed invention, and for at least this reason the rejection under 35 U.S.C. §102 is improper.

Mitra

Mitra describes, at column 7, lines 45-65:

“...Joining a secure multicast group requires the joining member first to set up a separate secure channel with the GSC of the group (using a unicast communication line). The purpose of the secure channel is to facilitate and isolate confidential communication between the GSC and this member during the time that the member is part of the group... Upon receiving a join request (and approving it), the GSC inserts the member's identification and information concerning the secure channel in a private database it maintains. In this way the GSC has full knowledge of the group membership and can communicate with each member separately and securely when required. The member must also store information concerning the secure channel for future communication with the GSC... All communications from the GSC must include a message digest and be digitally signed so that receivers may verify that the message has not been corrupted and the sender was actually the GSC... Only the GSC maintains information concerning group membership; members do not know about each other (except that receivers may need to know the list of authorized senders)...”

Mitra also states, at column 8, lines 14-22:

Serial No. 09/607007

- 25 -

Art Unit:2143

“...Once the GSC and the new member have authenticated each other and have agreed on a secret the GSC needs to provide the new member with information that will allow it to encrypt and/or decrypt the multicast transmission. At this point the GSC also needs to change the group key ( $K_{grp}$ ) which provides access to the multicast transmissions. This is done to prevent the joining member from decrypting previous transmissions to which it should not have access...”

Thus, in Mittra, when a device seeks to join a group:

- 1). The host establishes a separate side channel communication with the GSC.
- 2). Within the channel, the host issues a ‘join request’ to start authentication. In response to the ‘join’ request, the GSC starts the authentication process
- 3). When authenticated, the host receives a group key from the GSC
- 4). The host communicates within the group

In contrast to Mittra, the method of accessing a shared tree is described in the claims is, when the host device seeks to join a group:

- 1). The host establishes communication with a key server, where it obtains a token, the token being unique to the particular *host/group* pair;
- 2). To join the group, the host forwards a join request to a designated device for the group, the request including the token;
- 3). The designated device authenticates the host’s ability to join the group using the token, and then forwards key information to the host to permit the host to communicate within the group.

Applicant’s invention provides a fast way to ensure that a *host may validly issue join requests for a group*. This ability is not present in Mittra.

The Examiner states, at page 16 of the Office Action:

“... First, the applicant’s representative remark that the claimed invention possesses a key server, separate from the host. The examiner would like to point out that such means are also present within the Mittra prior art. Within column 4, lines 53-56, Mittra discloses that if desired, the design can be implemented with key distribution centers. Such devices are separate from the host. Additionally, since the key distribution centers provide a service to the clients (distribute keys), it is a form of a server...”

Applicant’s respectfully submit that the Examiner has misread and/or misinterpreted limitations of the claimed invention. Claim 1 recites that the “designated device... through

Serial No. 09/607007

- 26 -

Art Unit:2143

which the host device accesses the shared tree” is “separate from the key server”, thereby clearly separating the point of *authentication of the host* from the entry of the host into the tree. No such structure is shown or suggested by Mittra. In contrast, the authentication in Mittra occurs simultaneously with the joining of the tree.

The Examiner refers to Mittra’s statement that “Of course, well known, secure key distribution centers (KDCs) and certification authorities (CAs) may also be used as required by the security technology used to build a specific implementation of one of the protocols....” In determining how these could be used with Mittra, Applicants’ can only assume that these are used to obtain the keys or certificates in Mittra; the authentication of the host is still performed when the host joins the tree, wherever the key is obtained.

It would appear that the Examiner has not appreciated the patentable weight of the limitations of the claims. However, it should be appreciated that the present invention, by permitting a method to separately authenticate a host’s join requests overcomes a problem that is not capable of being overcome by Mittra; namely, join requests from unauthorized hosts will *not* be forwarded up the multicast tree for authentication processing. Mittra provides no such protection.

Thus there are several elements of claim 1 which are not recited in Mittra. In particular, Mittra neither describes nor suggests “a designated device, separate from the key server, through which the host device requests access to the shared tree associated with a group...” Rather Mittra provides authentication and key distribution from a *single* device. In addition, Mittra neither describes nor suggest “...the host device obtains access information from the key server for the host device to request access to the shared tree associated with the group, the access information including authentication information unique to the host device/group pair ...”

Serial No. 09/607007

- 27 -

Art Unit:2143

Rather, while Mitra does state that a side channel is established with the host device, no mention is made that authentication information used in the side channel is 'unique to the host device/group pair...'

Accordingly, for at least the reason that every limitation of claim 1 is neither described nor suggested in Mitra, the rejection under 35 U.S.C. §102 should be withdrawn. Independent claims 16, 28, 40, 61, 68, 75, 87, 99 and 122 have been amended to include limitations similar to those of claim 1 which assist to distinguish the claims over Mitra, and thus the rejection under 35 U.S.C. §102 for these claims should be withdrawn as well. Dependent claims 2-15, 17-27, 29-39, 41-60, 69-74, 76-86, 88-98, 100-121 and 122-144 serve to add further patentable limitations to their parent independent claims, but are allowable for at least the reason put forth above with regard to their parent independent claim.

Serial No. 09/607007

- 28 -

Art Unit:2143

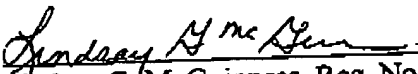
Conclusion

Applicants have made a diligent effort to place the claims in condition for allowance. However, should there remain unresolved issues that require adverse action, it is respectfully requested that the Examiner telephone Lindsay G. McGuinness, Applicants' Attorney at 978-264-6664 so that such issues may be resolved as expeditiously as possible.

For these reasons, and in view of the above amendments, this application is now considered to be in condition for allowance and such action is earnestly solicited.

Respectfully Submitted,

4/11/2005  
Date

  
Lindsay G. McGuinness, Reg. No. 38,549  
Attorney/Agent for Applicant(s)  
Steubing McGuinness & Manaras LLP  
125 Nagog Park Drive  
Acton, MA 01720  
(978) 264-6664

Docket No. 120-147  
Dd: 6/30/2004